UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/005,291	12/04/2001	Jing Zheng Ouyang	Inno-008	8092

29956 7590 06/16/2005

TIMOTHY P. O'HAGAN
8710 KILKENNY CT
FORT MYERS, FL 33912

EXAMINER	
PICH, PONNOREAY	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 06/16/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/005,291	OUYANG, JING ZHENG	
	Examiner	Art Unit	
	Ponnoreay Pich	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *04 December 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-17 and 19-21* is/are rejected.

7)☒ Claim(s) *18* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *04 December 2001* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *11-2002 and 8-2003*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claims 1-21 have been examined and are pending.

Priority

The examiner spoke with Mr. Timothy O'Hagan on 6/7/2005 over the telephone and confirmed that applicant's claim to priority application 09/632,696 was filed in error. Applicant is not entitled to an earlier effective filing date than the actual filing date of the application, which was 12/4/2001. **The examiner requests that applicant in the response to this office action respond in writing confirming the above statement so that the records concerning priority data for this application may be fixed.**

Information Disclosure Statement

The IDS submitted by the applicant have been considered.

Drawings

Figures 1a, 1b, and 2 should be designated by a legend such as --Prior Art-- because only that which is old is illustrated. See MPEP § 608.02(g). Corrected drawings in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. The replacement sheet(s) should be labeled "Replacement Sheet" in the page header (as per 37 CFR 1.84(c)) so as not to obstruct any portion of the drawing figures. If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

In applicant's specification, on page 6, lines 28-29, applicant discloses that Figure 1a is the cipher steps used for the AES algorithm. Page 7, lines 8-9 discloses

that Figure 1b is the inverse cipher step of the AES algorithm. Applicant disclosed also that the AES algorithm was already known before applicant's invention was made (p1, lines 11 and 20-23). As per Figure 2, applicant discloses that Figure 2 shows the MixColumns transform and InvMixColumns transform (p7, lines 16-17). Both these transforms were disclosed by the applicant as known before applicant invention was made and as being part of the AES algorithm (see specification p3, lines 20-25). Applicant did not disclose anywhere in the specification where there were anything in Figures 1a, 1b, or 2 that were improvements on the prior art on the part of the applicant.

Claim Objections

Claims 12 and 15 are objected to because of the following informalities: The examiner believes applicant meant to recite Galois **field** instead of Galois **filed** in both claims 12 and 15. Appropriate correction is required.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claim 4 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

As per claim 4, the examiner respectfully asks that applicant double check the wording of the claim as the examiner believes the applicant may have made a mistake in the wording which renders what exactly it is applicant is trying to claim unclear.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-4, 16-17, and 19 are rejected under 35 U.S.C. 102(e) as being anticipated by Rose (US 6,510,228).

Claim 1:

Rose discloses an improved method for encryption, comprising:

1. Receiving original data to be encrypted (Fig 2).
2. Performing cipher steps to process the original data into encrypted data, including:
    a. Looking up logs of terms being multiplied over a finite field (col 6, lines 60-67).
    b. Summing the logs to obtain a sum (col 6, lines 60-67).
    c. Looking up the anti-log of the sum (col 6, lines 60-67). Note exponent is the same as anti-log.
3. Outputting the encrypted data (Fig 2).

In Fig 2, data is encrypted, so at some point it must have been received by some means.

Claim 2:

Rose further discloses wherein looking up the anti-log of the sum comprises looking up the anti-log of the sum in the primitive power and log table (col 6, lines 60-67).

Claim 3:

Rose further discloses wherein looking up the anti-log of the sum comprises looking up the anti-log of the sum in the primitive power and log table (col 6, lines 60-67).

Claim 4:

Rose further discloses wherein the finite field is a Galois field (col 6, line 67-col 7, line 2).

Rose does not explicitly disclose looking up the log of terms in a primitive power and log table comprises looking up the log of terms in a primitive power and log table, of a primitive element of the Galois field. However, this limitation is inherent to Rose because a Galois field must have primitive elements, therefore the primitive power and log table must contain the log of primitive elements of the Galois field. When looking up terms in the table which involves the primitive element, the primitive element must be looked up in the table also.

Claim 16:

Rose discloses an improved method for encryption including multiplication over a finite field (col 6, line 60-col 7, line 2), the improvement comprising:

1. Obtaining the result of multiplication over the finite field using a primitive power and log table comprising 2 rows (col 6, lines 13-22 and columns 7-8, Tables 1 and 2).

Claim 17:

Rose further discloses wherein obtaining the result of multiplication over a finite field comprises:

1. Looking up logs of terms being multiplied over the finite field (col 6, lines 60-67).
2. Summing the logs to obtain a sum (col 6, lines 60-67).
3. Looking up the anti-log of the sum (col 6, lines 60-67).

Claim 19:

Rose further discloses wherein the primitive power and log table is based on a primitive is selected from the set consisting of the 128 primitives of the Galois field(2^8) (col 6, lines 23-41).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 5-15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rose (US 6,510,228) in view of applicant's admittance of prior art.

Claim 5:

Rose does not disclose wherein:

1. The encryption utilizes the AES algorithm, wherein the AES algorithm includes a Cipher and an Inverse Cipher, and wherein the Cipher includes a MixColumns transform, and wherein the Inverse Cipher includes an InvMixColumns transform; and
2. Looking up the log of terms being multiplied comprises looking up the logs of terms being multiplied over a finite field in the MixColumns transform of the Cipher and in the InvMixColumns transform of the Inverse Cipher.

However, the AES algorithm was well known to one of ordinary skill in the art at the time the applicant's invention was made. Applicant further disclosed this in applicant's specification (p1, lines 20-23). The limitations recited above are inherent to the AES algorithm as the National Institute of Standards and Technology (NIST) choose Rijndael's algorithm as the AES algorithm on October 2, 2000.

In light of the above, it would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to have modified Rose's invention according to the limitations recited in claim 5 by using the AES algorithm. One of ordinary skill would have been motivated to do so as the AES algorithm is the current

encryption standard officially recognized by the NIST and is used to protect sensitive government data.

Claim 6:

Rose does not disclose the wherein looking up the logs of terms being multiplied over a finite field in the MixColumns transform of the Cipher and in the InvMixColums transform of the Inverse Cipher comprises looking up the logs of the terms being multiplied over a Galois field in the MixColumns transform of the Cipher and in the InvMixColumns transform of the Inverse Cipher. However, this limitation was disclosed by applicant as being part of the AES algorithm (p3, last paragraph and p4, first paragraph), therefore is a part of Rose's modified invention.

Claim 7:

Rose further disclose wherein looking up the log of terms being multiplied over a finite field comprises looking up the log of terms being multiplied over a Galois field (col 6, lines 13-22).

Claim 8:

Rose further discloses wherein looking up the log of terms comprises looking up the log of terms in a table comprising 2 rows (columns 7-8, Tables 1 and 2).

Claim 9:

Rose does not explicitly disclose transmitting the encrypted data, receiving the encrypted data, and outputting the original data. However, Rose discloses that encryption is a process whereby data is manipulated by a random process such that the data is made unintelligible by all but the targeted recipient (col 1, lines 12-14). As such,

the above limitations must exist in Rose's invention since Rose's invention relates to encryption.

Rose also does not disclose performing Inverse Cipher steps including:

1. Looking up the log of the terms being multiplied over the finite field.
2. Summing the logs to obtain a sum.
3. Looking up the anti-log of the sum.

However, the AES algorithm was well known to one of ordinary skill in the art at the time the applicant's invention was made. Applicant further disclosed this in applicant's specification (p1, lines 20-23). The above limitations are inherent to the AES algorithm. It would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to have modified Rose's invention according to the limitations recited in claim 9 by utilizing the AES algorithm. One of ordinary skill would have been motivated to do so for the same reasons given in claim 5.

Claim 10:

Rose discloses an encryption system comprising:

1. A first communication device adapted to receive original data (Fig 2) and including:
    a. Means for encrypting the original data to generate encrypted data including:
        i. Means for looking up logs of terms being multiplied over a finite field (col 6, lines 60-67).

ii. Means for summing the logs to obtain a sum (col 6, lines 60-67).

iii. Means for looking up the anti-log of the sum (col 6, lines 60-67).

iv. Means for outputting the encrypted data (Fig 2).

Rose does not disclose means for performing a MixColumns transform. However, applicant disclosed in the specification that the AES algorithm was well known at the time the applicant's invention was made including the use of a MixColumns transform as part of the AES algorithm (p1, lines 20-23 and p3, lines 20-21). In light of this, it would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to have modified Rose's invention according to the limitations recited in claim 10 by utilizing the AES algorithm. One of ordinary skill would have been motivated to do so for the same reasons given in claim 5.

Claim 11:

Rose further discloses the means for encrypting the original data comprises a processor (Fig 2, item 22). Rose does not disclose the processor adapted to exercise the AES algorithm. However, applicant disclosed the AES algorithm as known at the time the applicant's invention was made (p1, lines 20-23). It would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to have further modified the modified invention of Rose according to the limitation recited in claim 11. One of ordinary skill would have been motivated to do so for the same reasons given in claim 5.

Claim 12:

Rose further discloses wherein the finite field is a Galois field (2^8) (col 6, line 67-col 7, line 2).

Claim 13:

Claim 13 is substantially similar to claim 9 and is rejected for the same reasons and motivations. The differences are that claim 13 recites an inverse encryption system with means for performing the method of claim 9 including a second communication device, which was not mentioned in claim 9. However, it is obvious that there must be a second communication device to receive the encrypted data transmitted as recited in claim 9.

Claim 14:

Claim 14 is rejected for the same reasons as claim 11.

Claim 15:

Claim 15 is rejected for the same reasons as claim 12.

Claim 20 is rejected under 35 U.S.C. 103(a) as being unpatentable over Rose (US 6,510,228) in view of common practice in the art.

Claim 20:

Rose does not explicitly disclose wherein the improvement is implemented in C code. However, C code being used in encryption system is well known and one of ordinary skill and would be motivated to use C code to implement the improvement

because it is a commonly used programming language preferred by many engineers and computer scientists. Functions implemented in C also tend to be relatively fast.

Claim 21 is rejected under 35 U.S.C. 103(a) as being unpatentable over Rose (US 6,510,228) in view of Hung et al (Us 6,263,470).

Claim 21:

Rose does not explicitly disclose wherein the improvement is implemented in assembly code in a Digital Signal Processing (DSP) chip. However, coding in assembly is well known and it is the lowest level language still understandable by humans. One of ordinary skills would be motivated to use codes implemented in assembly because assembly gives full access to computer hardware, whereas higher-level languages tend to implement some level of hardware protection to prevent direct user access. Further, Hung discloses use of a DSP chip (col 3, line 66-col 4, line 6). One of ordinary skill would be motivated to implement a DSP chip in Rose's encryption invention because Hung discloses that DSP chips are generally favored in modern data processing and communication applications (col 3, line 66-col 4, line 6).

In light of the above, it would have been obvious to one of ordinary skill in the art to modify Rose's invention according to the limitations recited in claim 21. One of ordinary skill would have been motivated to do so for the reasons given above.

Allowable Subject Matter

Claim 18 is objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

As per claim 18, the examiner did not find in the prior art teachings or suggestions of obtaining the result of multiplication over a finite field comprises obtaining the result of multiplication over a Galois field(2^8) performed in the MixColumns transformation and in the InvMixColumns transformation of the AES algorithm, *using a 2 by 256 primitive power and log table.*

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ponnoreay Pich whose telephone number is 571-272-7962. The examiner can normally be reached on 8:00am-4:30pm Mon-Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Primary Examiner
Art Unit 2135

PP